



TRINKFON KİTLE FONLAMA PLATFORMU A.Ş

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Sürüm 1- 25/12/2023 tarihinde alınan 2023/01 sayılı Yönetim Kurulu kararıyla kabul edilmiştir ve kararın alındığı tarih itibariyle yürürlüğe girmiştir.

Sürüm 2- 29/07/2024 tarihinde alınan 2024/03 sayılı Yönetim Kurulu kararıyla revize edilmiştir.

1. Bu politikanın amacı, 6698 sayılı Kişisel Verilerin Korunması Kanununa (Kanun) uygun olarak tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.
2. Bu politika; 6698 sayılı Kanunun 7.nci maddesinin üçüncü fıkrası ile 22.nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış 28/10/2017 tarihli Resmî Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliğine uygun olarak hazırlanmıştır.
3. Şirket; Kişisel veri işleme envanterine uygun olarak bu kişisel veri saklama ve imha politikasını hazırlamıştır.
4. **Tanımlar**
 - 4.1. **Alıcı grubu:** Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.
 - 4.2. **İlgili kullanıcı:** Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişilerdir
 - 4.3. **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

- 4.4. Kayıt ortamı:** Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı ifade eder.
- 4.5. Kişisel veri işleme envanteri:** Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanterdir.
- 4.6. Kişisel veri saklama ve imha politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.
- 4.7. Periyodik imha:** Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi ifade eder.
- 4.8. Sicil:** Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.
- 4.9. Veri kayıt sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
- 4.10. Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
- 4.11. Kişisel verilerin silinmesi** Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
- 4.12. Kişisel verilerin yok edilmesi** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.
- 4.13. Kişisel verilerin anonim hale getirilmesi** Kişisel verilerin başka verilerle eşleştirilirse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişi ile ilişkilendirilemez hale getirilmesi gerekir.

5. Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamları:

5.1. Kâğıt ortamlar

5.1.1. Kâğıt

5.1.2. Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)

5.1.3. Yazılı, basılı, görsel ortamlar

5.2. Elektronik ortamlar

5.2.1. Sunucular (Etki alanı, yedekleme, e-posta,

5.2.2. Veritabanı, web, dosya paylaşım, vb.)

5.2.3. Yazılımlar

5.2.4. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)

5.2.5. Kişisel bilgisayarlar (Masaüstü, dizüstü)

5.2.6. Mobil cihazlar (telefon, tablet vb.)

5.2.7. Optik diskler (CD, DVD vb.)

5.2.8. Çıkarılabilir bellekler (USB, Hafıza Kart vb.)

5.2.9. Yazıcı, tarayıcı, fotokopi makinesi

6. Saklamayı Gerektiren Hukuki Sebepler

6.1. 6698 sayılı Kişisel Verilerin Korunması Kanunu,

6.2. 6098 sayılı Türk Borçlar Kanunu,

6.3. 4734 sayılı Kamu İhale Kanunu,

6.4. 657 sayılı Devlet Memurları Kanunu,

6.5. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

6.6. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar

6.7. Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

6.8. 5018 sayılı Kamu Mali Yönetimi Kanunu,

6.9. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,

6.10. 4982 Sayılı Bilgi Edinme Kanunu,

6.11. 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun

- 6.12.** 4857 sayılı İş Kanunu,
- 6.13.** 2547 sayılı Yükseköğretim Kanunu,
- 6.14.** 5434 sayılı Emekli Sağlığı Kanunu,
- 6.15.** 2828 sayılı Sosyal Hizmetler Kanunu
- 6.16.** İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- 6.17.** Arşiv Hizmetleri Hakkında Yönetmelik
- 6.18.** Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

7. Saklamayı Gerektiren İşleme Amaçları

- 7.1.** Acil Durum Yönetimi Süreçlerinin Yürütülmesi
- 7.2.** Bilgi Güvenliği Süreçlerinin Yürütülmesi
- 7.3.** Çalışan Adayı / Stajyer / Öğrenci Seçme ve Yerleştirme Süreçlerinin Yürütülmesi
- 7.4.** Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
- 7.5.** Çalışan Memnuniyeti ve Bağlılığı Süreçlerinin Yürütülmesi
- 7.6.** Çalışanlar İçin İş Akdi ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
- 7.7.** Çalışanlar İçin Yan Haklar ve Menfaatleri Süreçlerinin Yürütülmesi
- 7.8.** Denetim / Etik Faaliyetlerinin Yürütülmesi
- 7.9.** Eğitim Faaliyetlerinin Yürütülmesi
- 7.10.** Erişim Yetkilerinin Yürütülmesi
- 7.11.** Faaliyetlerin Mevzuata Uygun Yürütülmesi
- 7.12.** Finans ve Muhasebe İşlerinin Yürütülmesi
- 7.13.** Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
- 7.14.** Fiziksel Mekân Güvenliğinin Temini
- 7.15.** Görevlendirme Süreçlerinin Yürütülmesi
- 7.16.** Hukuk İşlerinin Takibi ve Yürütülmesi
- 7.17.** İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
- 7.18.** İletişim Faaliyetlerinin Yürütülmesi

- 7.19.** İnsan Kaynakları Süreçlerinin Planlanması
- 7.20.** İş Faaliyetlerinin Yürütülmesi / Denetimi
- 7.21.** İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
- 7.22.** İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması ve Değerlendirilmesi
- 7.23.** İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- 7.24.** Lojistik Faaliyetlerinin Yürütülmesi
- 7.25.** Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
- 7.26.** Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
- 7.27.** Mal / Hizmet Satış Süreçlerinin Yürütülmesi
- 7.28.** Mal / Hizmet Üretim ve Operasyon Süreçlerinin Yürütülmesi
- 7.29.** Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
- 7.30.** Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
- 7.31.** Organizasyon ve Etkinlik Yönetimi
- 7.32.** Pazarlama Analiz Çalışmalarının Yürütülmesi
- 7.33.** Performans Değerlendirme Süreçlerinin Yürütülmesi
- 7.34.** Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
- 7.35.** Risk Yönetimi Süreçlerinin Yürütülmesi
- 7.36.** Saklama ve Arşiv Faaliyetlerinin Yürütülmesi
- 7.37.** Sosyal Sorumluluk ve Sivil Toplum Aktivitelerinin Yürütülmesi
- 7.38.** Sözleşme Süreçlerinin Yürütülmesi
- 7.39.** Sponsorluk Faaliyetlerinin Yürütülmesi
- 7.40.** Stratejik Planlama Faaliyetlerinin Yürütülmesi
- 7.41.** Talep / Şikayetlerin Takibi
- 7.42.** Taşınır Mal ve Kaynakların Güvenliğinin Temini
- 7.43.** Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
- 7.44.** Ücret Politikasının Yürütülmesi
- 7.45.** Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi

- 7.46. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
- 7.47. Yabancı Personel Çalışma ve Oturma İzni İşlemleri
- 7.48. Yatırım Süreçlerinin Yürütülmesi
- 7.49. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
- 7.50. Yetkili Kişi, Kurum ve Kuruluşlara Bilgi Verilmesi
- 7.51. Yönetim Faaliyetlerinin Yürütülmesi
- 7.52. Ziyaretçi Kayıtlarının Oluşturulması ve Takibi

8. İmhayı Gerektiren Sebepler

- 8.1. Kişisel verilerin işleme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.
- 8.2. Türk Ceza Kanunu'nun 138. maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Şirket kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir.
- 8.3. İlgili kişi, Şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.
- 8.4. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.
- 8.5. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.
- 8.6. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.
- 8.7. Kişisel verilerin saklanması gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması
- 8.8. Kişisel verinin işlenmesine esas olan mevzuat hükümlerinin değişmesi veya ilgası

9. Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler

- 9.1.1.** Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- 9.1.2.** Ağ yoluyla veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- 9.1.3.** Anahtar yönetimi uygulanmaktadır.
- 9.1.4.** Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- 9.1.5.** Çalışanlar için yetki matrisi oluşturulmuştur.
- 9.1.6.** Erişim logları düzenli olarak tutulmaktadır.
- 9.1.7.** Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
- 9.1.8.** Gerektiğinde veri maskeleyme yöntemi uygulanmaktadır.
- 9.1.9.** Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- 9.1.10.** Kişisel veri güvenliğinin takibi yapılmaktadır.
- 9.1.11.** Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- 9.1.12.** Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- 9.1.13.** Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- 9.1.14.** Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- 9.1.15.** Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- 9.1.16.** Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- 9.1.17.** Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- 9.1.18.** Mevcut risk ve tehditler belirlenmiştir.
- 9.1.19.** Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

- 9.1.20. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
- 9.1.21. Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- 9.1.22. Sızma testi uygulanmaktadır.
- 9.1.23. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
- 9.1.24. Şifreleme yapılmaktadır.
- 9.1.25. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklara denetimi sağlanmaktadır.
- 9.1.26. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
- 9.1.27. Veri kaybı önleme yazılımları kullanılmaktadır.
- 9.1.28. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- 9.1.29. Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- 9.1.30. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.
- 9.1.31. Gizlilik taahhütnameleri yapılmaktadır.
- 9.1.32. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- 9.1.33. Kâğıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- 9.1.34. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- 9.1.35. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- 9.1.36. Kişisel veriler mümkün olduğunca azaltılmaktadır.
- 9.1.37. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- 9.1.38. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler mevcuttur.

10. Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler

- 10.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılır ve kayıt altına alınır.
- 10.2. Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

11. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Teknikleri

Kişisel Verilerin Silinmesi

Sunucularda Yer Alan Kişisel Veriler: Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

12. **Elektronik Ortamda Yer Alan Kişisel Veriler:** Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

12.1. Fiziksel Ortamda Yer Alan Kişisel Veriler Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır. Örnek: İlgili dosyanın, belgenin parçalanarak çöpe atılması.

12.2. Yazılımdan Güvenli Olarak Silme Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; çok yüksek ihtimalle bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

12.3. Uzman Tarafından Güvenli Olarak Silme Şirket bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

Kişisel Verilerin Yok Edilmesi

12.4. Fiziksel Ortamda Yer Alan Kişisel Veriler: Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

12.5. Optik / Manyetik Medyada Yer Alan Kişisel Veriler: Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

12.6. Kişisel Verileri Anonim Hale Getirme Teknikleri

- 12.6.1.** Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Şirket, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.
- 12.6.2.** KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemler KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.
- 12.6.3. Maskeleye (Masking)** Veri maskeleye, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, T.C Kimlik No, ad, soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkansız hale geldiği bir veri setine dönüştürülmesi.
- 12.6.4. Toplulaştırma (Aggregation)** Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.
- 12.6.5. Veri Türetme (Data Derivation)** Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehrin belirtilmesi.
- 12.6.6. Veri Karma (Data Shuffling, Permutation)** Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

13. Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimleri ve görev tanımları:

- 13.1. Bilgi İşlem Birimi Yöneticisi;** Şirketin tüm Bilgi İşlem süreçlerini yönetir.
- 13.2. İnsan Kaynakları Yöneticisi (Personel ile ilgili konularda),** Şirketin tüm personel süreçlerini yönetir.

13.3. Satış ve Pazarlama Yöneticisi (Müşteri bilgileri ile ilgili konularda); Şirketin tüm satış pazarlama süreçlerini yönetir.

14. Saklama ve imha sürelerini gösteren tablo

NO	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
1	Kimlik	15 YIL
2	İletişim	15 YIL
3	Lokasyon	2 YIL
4	Özlük	15 YIL
5	Hukuki İşlem	10 YIL
6	Müşteri İşlem	5 YIL
7	Fiziksel Mekân Güvenliği	2 YIL
8	İşlem Güvenliği	2 YIL
9	Risk Yönetimi	10 YIL
10	Finans	10 YIL
11	Mesleki Deneyim	15 YIL
12	Pazarlama	5 YIL
13	Görsel ve İşitsel Kayıtlar	15 YIL
18	Sağlık Bilgileri	15 YIL
19	Ceza Mahkûmiyeti ve Güvenlik Tedbirleri	15 YIL

***Yukarıdaki süreler, çalışanlar için iş sözleşmesinin feshi tarihinden, tedarikçi ve müşteriler için sözleşmenin sona erme tarihinden veya sözleşme yoksa son işlemin yapıldığı tarihten, diğer ilgili kişiler için kişisel verilerin elde edilme tarihinden itibaren başlar.**

15. Periyodik imha süreleri,

- 15.1.** Şirket saklama süresi dolan kişisel verileri saklama süresinin dolduğu tarihten itibaren en geç 180 gün içerisinde imha eder.
- 15.2.** Şirket; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.
- 15.3.** Periyodik imhanın gerçekleştirileceği zaman aralığı veri sorumlusu tarafından kişisel veri saklama ve imha politikasına, prosedürlere ve şirketin iş akışına uygun olarak belirlenir. Bu süre her halde altı ayı geçemez.

16. Politikanın Yayınlanması ve Saklanması

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır.

17. Güncelleme Periyodu

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

18. Yürürlük

Politika, Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

19. Veri Sorumlusu:

Veri Sorumlusu Unvan	: Trinkfon Kitle Fonlama Platformu A.Ş.
Mersis No	: 0859142576500001
E-posta Adresi	: info@trinkfon.com
Kayıtlı Elektronik Posta Adresi	: trinkfon@hs01.kep.tr
Fiziki Posta Adresi	: Gökkuşuğı Mah. 1204 Cad. Acar Apt. No:19/20 Çankaya, Ankara

EK- 1: İLGİLİ KİŞİNİN TALEBİ ÜZERİNE İMHA TUTANAĞI:**İLGİLİ KİŞİ TALEBİ ÜZERİNE DOKÜMAN İMHA TUTANAĞI**

Aşağıda listelenmiş olan kişisel ve özel nitelikli kişisel veriler içeren dokümanlar, **Veri Sorumlusu** sıfatıyla **Trinkfon KİTLE FONLAMA PLATFORMU A.Ş.** tarafından; 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat uyarınca, ilgili kişinin talebi doğrultusunda kişisel verilerin imha edilmesi gerçekleştirilmiştir. İlgili kişinin talebi doğrultusunda imha edilen dokümanlarla ilgili kullanılan imha tekniği ve tarihi, imha edilen dokümanların ve dosyaların içeriği aşağıdaki tablolarda detaylı olarak belirtilmiştir.

İlgili Kişi	
İlgili Kişi İmha Talep Tarihi	
İmha Tekniği	
İlgili Kişiye İmha Evrakı Tebliğ Tarihi	
Dokümanlarda Bulunan Veri Kategorileri	(Kimlik, iletişim, finans, mesleki deneyim, görsel işitsel kayıtlar vb.)
Dokümanların Bulunduğu Ortam	(Fiziki ise özlük dosyası, sanal ise Google Drive/Cloud vb.)

İmha Edilen Doküman Listesi	
1.	2.
3.	4.
5.	6.
7.	8.
9.	10.
11.	12.
13.	14.
İMHA EDEN Adı Soyadı / Pozisyon / İmza	İMHAYA TANIK OLAN Adı Soyadı / Pozisyon / İmza

EK 2- PERİYODİK İMHA TUTANAĞI:

Aşağıda listelenmiş olan kişisel ve özel nitelikli kişisel veriler içeren dokümanlar, **Veri Sorumlusu** sıfatıyla **Trinkfon KİTLE FONLAMA PLATFORMU A.Ş.** tarafından; 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat uyarınca, kişisel ve özel nitelikli kişisel veriler içeren dokümanların **Kişisel Veri Saklama ve İmha Politikası** uyarınca **saklama sürelerinin bitmesi nedeniyle** imha edilmesi gerçekleştirilmiştir. Yasal saklama sürelerinin bitmesi doğrultusunda imha edilen dokümanlarla ilgili kullanılan imha tekniği ve tarihi, imha edilen dokümanların ve dosyaların içeriği aşağıdaki tablolarda detaylı olarak belirtilmiştir.

Verileri imhaya Konu İlgili Kişi	
İmha Tarihi	
Kullanılan İmha Tekniği	
Dokümanlarda Bulunan Veri Kategorileri	(Kimlik, iletişim, finans, mesleki deneyim, görsel işitsel kayıtlar vb.)
Dokümanların Bulunduğu Ortam	(Fiziki ise özlük dosyası, sanal ise Google Drive/Cloud vb.)

İmha Edilen Doküman Listesi	
1.	2.
3.	4.
5.	6.
7.	8.
9.	10.
11.	12.
13.	14.
İMHA EDEN Adı Soyadı / Pozisyon / İmza	İMHA YAPAN Adı Soyadı / Pozisyon / İmza

Bu Politika, Trinkfon Kitle Fonlama Platformu A.Ş. Yönetim Kurulu'nun 25/12/2023 tarih ve 2023/01 sayılı kararı ile onaylanmıştır ve aynı gün yürürlüğe konmuştur.

İşbu politika Trinkfon Kitle Fonlama Platformu A.Ş. Yönetim Kurulu tarafından 29/07/2024 tarihinde alınan 2024/03 sayılı kararla revize edilmiştir.

Trinkfon Kitle Fonlama Platformu A.Ş.

Mersis No :0859142576500001

Gökkuşığı Mah. 1204 Cad. Acar Apt. No: 19/20 Çankaya / Ankara info@trinkfon.com